OKW/Chi Cryptanalytic Research on

Enigma, Hagelin and Cipher Teleprinter Machines.

The attached papers, written jointly by ORR HUETTENHAIN and Sdf. Dr. FRICKE at the request of TICOM, cover OKW/Chi methods of solution of the Enigma and the Hagelin C-36 and BC-38 machines; and the cipher teleprinters T 52 a/b, T 52/c, SFMT 43, SZ 40 and SZ 42 a/b.

TICOM
1st Aug. 1945

No. of pages 19
Copy No. 16

Distribution

British
1 Director
2 D.D.3
3 D.D.4
4 D.D.(N.S.)
5 D.D.(MW)
6 D.D.(A.S.)
7-8 A.D.(C.C.R.)(2)
9 Col. Leathem

TICOM
10 Chairman
11-12 S.A.C.(2)
13 Cdr. Bacon
14 Cdr. MacKenzie
15 Cdr. Tandy
16 Lt.Col. Johnson
17 Major Seaman
18 Lt. Eachus
19 Lt. Vance
20 Capt. Cowan
21 Lt. Fehl
22-23 Ticom Files (2)
24 Cdr. Manson

U.S.
25-26 OP20-G(2)(via Lt. Pendergrass)
27 G-2(via Lt.Col. Hilles)
28-29 S.S.A.(2)(via Major Seaman)
30 Director, S.I.D. ETOUSA (via Lt.Col. Johnson)

Additional
31 Major Morgan
32 A.D.(Mch)

SOLUTIONS OF ENIGMA MACHINES

(1) K Machines

(a) Elementary Solution

In the case of Enigma K a Spaltencäsar of period $26x26^3 = 440,000$ is deduced. On account of the six wheel orders a total of six periods of this length exist. The substitutions are reciprocal.

If 20 to 25 messages of the same setting are available then the solution of these messages can be done in an elementary manner i.e. the columns of the encoded texts written under one another in depth are solved as a Spaltencäsar. In this the reciprocity of the substitutions is made use of to a great extent. In the solution procedure no other characteristic of the machine is used. This is also valid for the elementary solution of Stecker Enigma. After this elementary solution of the encoded texts the determination of the machine setting presents no difficulties. This is an easier problem than the solution from part compromise (Teilkompromiss) which is described in (b).

(b) Solution from a Part Compromise

The knowledge of how the machine works and the circuit of the wheels is assumed. The solution is as follows:-

Since the middle wheel only makes one step for every 26 letters, then the middle wheel, the left wheel and the Umkehr wheel together can be regarded for this period of time as a fixed Umkehr wheel. In figure 1 (see appendix) everything left of the red line is considered as an Umkehr wheel. The terminals of the wires from the 26 keys of the keyboard through the entrance wheel (Eingangswalze) are fixed. For every letter the right wheel moves one step. Since the circuit of the wheels for each of the 26 different positions of the right wheel are presumed known, the position at which all the 26 letters end at the red line can be stated. The turning of the right wheel can therefore be made ineffective. If a short clear - encoded compromise (Klar-Geheim-Kompromiss) is available then the terminals of the clear letters and the corresponding encoded letters at the red line can be marked for each of the three wheels in each of the 26 positions (any one of these wheels can appear as the right wheel). Under the $3x26 = 78$ different markings such a wheel must appear which will not contradict the assumption of a large Umkehr wheel left of the red line.

Example: Given the following compromise:

Clear text: g a b i n e t t o a l t

encoded text: z s e w g j i x j p s u

The circuit of a wheel is given in figure 2 (see appendix) column 1. This is to be understood as follows:

any contact(Stift) of the wheel is taken as zero point for counting. Then the wire which goes into the wheel at this zero point is connected in such a way that it comes out at point 6. The second wire terminates at point 12. The third wire at point 1 etc. Zero point for counting is however chosen in such a way that when A is typed it is in such a position that it will lie opposite the terminal of key A in the entrance wheel. In other words: when key F is pressed the current ends at the red line at position 9 etc. The second column of figure 2 gives the positions at the red line when the right wheel has moved one step etc.

A table as in figure 2 must be worked out for each of the three wheels.

After these preparations a compromise is investigated. Figure 3 (see appendix) results. Under the clear text and corresponding encoded text in accordance with each of the three tables 26 rows of figures are written for each of the three wheels. The first line under the clear text results as follows: In figure 2 near g in the first column is 14, near a in the second column is 11, near b in the third column is 06. In this way originates the first line under the encoded text. The second line of figure 3 gives the numbers which are next to g in the second and next to A in the third column etc. Now the horizontal rows of figures are investigated:

1) If there are two similar numbers in one clear text row of figures then in the encoded text row of figures at the same positions there must also be two similar numbers(but not the same ones), and vice versa.

2) In a clear text row of figures if there is a number which also appears at another position in the encoded text row of figures then the numbers which are at corresponding positions in the neighboring rows of figures must also be equal.

3) At no position in neighboring rows of figures at the same position must there be similar numbers.

In all 3 x 26 pairs of rows the solution is provided by the pair for which the three conditions are fulfilled. This is fulfilled in the example in Fig. 3 in the third row of figures. In this way the right wheel of the three wheels is determines. In addition its initial position at the beginning of the part compromise is determined, in the example therefore 3. If during the encoding the center wheel has moved one step, then the three conditions mentioned above are no longer valid for all the rows of figures of Fig. 3. The conditions are fulfilled sepa rately for a left and a right part of the rows of figures.

In this case the center wheel and its initial position can then be determined according to the same principle. The red line of Fig.1 is moved the breadth of one wheel to the left.

The initial position of the left wheel still remains to be determined. For this 26 attempts are nedessary, which can be carried out in a very short time.

If, however, the center wheel does not move a step during the encoding of the compromise, then the center and the right wheels must be worked out systematically. Once an Umkehrwheel catalogue has been produced this work is rendered easier.

It is then no longer a problem to determine the Ringstellung of the wheels.

If in an encoded text a certain word is assumed at any one unknown position , then this word is "moved along" the entire encoded text in the manner just described. At the correct position the three conditions are again fulfilled in the row of figures.

c) Solution with the aid of the e-Leiste

With the K-machine six different wheel orders are possible. The adjustable Umkehr wheel can be set in twenty-six different positions. The perios of the three moveable wheels is about 17,000 steps. There are therefore 6 x 26 = 156 different periods of 17,000 long respectively possible . If in each of the 156 different periods the clear letter e is encoded 17,000 times, then 156 rows of encoded elements results, each 17,000 long. All these rows of encoded elements are designated e-Leiste.

The clear letter e appears in German with a frequency of 18%. If a German clear text encode with the K-machine is moved through the e-Leiste and if in each position the corresponding encoded elements are counted, then the correct phase position will have the maximum cases of correspondence. In this the Ringstellung need not be considered. The e-Leiste need only be prepared once. The comparison of the encoded text with the e-Leiste would have to be carried out on a machine. In order to come to a positive conclusion in a reasonable time, then several machines would have to be used at the same time, even if one machine was capable of making 10,000 comparisons per second.

In GERMANY a practical solution with the aid of the e-Leist was not carried out, as in practice the method of solution from a part compromise was always possible.

2) Stecker-Enigma

a) General remarks

Stecker-Enigma was considered secure when used according to regulations. In any case, in practice Stecker)Enigma was never solved. This, however, does not exclude the fact that in practice conditions could be available which provided the prerequisites for a solution; stereotyped beginnings, messages of the same phase, routing messages, etc. No clear texts and encoded texts, however were made available to PW by any branch of the Armed Forces, with which they could have attempted a practical solution, because these were always encoded according to regulations laid down. Only theoretical investigations therefore of the security of Stecker-Enigma were carried out. PW have ideas of how a solution could be made. In 1939 or 1940 regulations were replaced by better ones. At the same time the number of Stecker was also increased. To sum up the following must be stated: Although there are no facts available to enable PW to conjecture a practical solution, PW never lost the feeling of uncertainty. Therefore "Lückenfüllerwälze","Steckeruhr" and "Gerät 39" were developed. It was clear that if a solution were possible then the uniform movement of the wheels would be the starting point for the solution.

It should now be stated why the alteration of the regulations was necessary in 1939 and 40. This will be followed by ideas of how a solution could be made. Investigations concerning this had not been concluded by the spring; there was therefore still no report about this. These remarks therefore can only be short and they must also be considered critically.

b) Solution of Stecker-Enigma owing to faulty indicator technique .

Before 39 or 40 the following regulation for forming an indicator existed: With the day-key (Steckerverbindungen, Walzenlage, Ringstellungen) a "Grundstellung" of the three wheels was issued. In this "Grundstellung" a group of three letters which gave the actual initial position of the wheels when encoding the message was typed twice, one after the other. The result-six letters therefore-was incorporated at the head of the message as indicator. If therefore all indicators for one day were written under one another, then a Spaltenchiffer of six substitutions resulted in which in each case the first and fourth encoded letter from the same clear letter (but different from the first and fourth) and also the third and sixth encoded letter from the same clear letter (again also different from the others). In addition at that time only 4 to 6 Stecker connections were used.

These indicators and therefore the "Grundstellung" of all messages could now be solved as follows: All the 6 x 17,000 substitutions were tabulated without Stecker Connections. From these tables bigrams were formed according to the following rule: Each letter of the table appeared as the first letter of the bigrams: the second letter of the bigram was the letter of the table three letters distant in the same horizontal line, i.e. resulting from the same clear letter. The bigrams were listed alphabetically together with their origin-clear letter, wheel position, "Grundstellung". On the average therefore each of the 676 bigrams appeared 6 x 676 times.

Only a small amount of work was necessary to find from these tables the "Grundstellung" which had been used to form the indicators. This method was only possible because the small number of Stecker connections used meant that a considerable number of letters had not been affected at all.

Simultaneous with changing the indicator regulation, the number of Stecker connections was increased to 10.

No further alterations were made.

c) Ideas on the general solution of Stecker-Enigma.

The solution of K-machine with the aid of e-Leiste had been stated. It would be reasonable to assume that these ideas would be used for Stecker-Enigma to solve an individual message.

The effect of the stecker board can be indicated as follows: While the connection of the keys to the 26 terminals of the entrance wheel without Stecker connections is fixed, then when Stecker connections are used a permutation of the connection of keys to the entrance terminals results. The e-key is therefore not fixed to the e-terminal; the e-key can ve connected with any of the entrance terminals.

If therefore the principle of the e-Leiste is to be used to solve Stecker-Enigma, then 26 Leisten will have to be prepared; one Leiste for every letter from A to Z, each without Stecker connections.

The encoded text can, however, not becompared with these Leiste to see wheterer elements correspond; for, by Stecker connections which were used in the encoding of the encoded text, the terminals from the wheels to the ekys were altered.

In the case of Stecker-Enigma therefore the 26 most frequent bigrams must be recognised which appear instead of the same letters under onother as in the case of the K-machine.

Since a total of 676 different bigrams appear, then the message in which, by comparison with the letter Leisten, the26 most frequent bigrams are to be found, must be fairly long. It is not possible to state accurately how long, it must certainly run into thousands. The difficulty is as stated to find the 26 most frequent bigrams.

It is possible that these bigrams will be found more easily if several messages of the same phase are investigated instead of one long message. The length of this material which will consist of parts arranged in phases will have to be about 1,000 elements.

The investigations, as already stated, were never concluded, and it is impossible to state whether, from these considerations a solution of Stecker-Enigma would have resulted which would have been practical.

army did not according to OKW-190

SOLUTION OF HAGELIN MACHINES

1- Solution of Messages of the same phase in the case of C.36

All types of Hagelin machines work according to the same basic principle. There are 26 different substitutions available. These substitutions are known. They are built up systematically so that when an encoded element of the substitution is solved all other encoded elements of this substitution are also solved. This equals encoding of the clear text with the aid of one time pad Mod. 26.

The result of this fact is that two encoded texts of the same phase can always be solved. Both encoded texts are written underneath one another in the same phase. Each of the 2 encoded elements listed underneath one another is obtained by adding the same number to the two clear letters. There are therefore 26 different possibilities. If the 26 possible clear pairs for each pair of encoded elements listed under one another are written under one another, then from each column the pairs which give a clear text in the top and bottom lines must be found and arranged in rows.

The finding of the corret clear text pairs can be made essentially quicker and easier if once and for all a catalogue is made which contains, listed according to the frequency of their appearance in the language concerned, the 26 possible clear pairs for each encoded pair.

If the encoded texts are solved in this way then withe C.36 the peg arrangement of the wheels and thus the day key can be established from the row of figures of the shifts from clear to encoded elements. In this the fact that all peg wheels move uniformly i.e. that there are short sub periods according to the length of the periods of the individual wheels is made use of to a decisive extent.

Messages of the same phase are recognised by the following:-
1. By indicators
2. By parallel positions (parallelstellen) which appearl
3. By the maximum of similar elements resulting when the two messages are placed under one another in phase.

For 2 and 3 it is expedient to employ the corresponding deciphering machines,(Entzifferungshilfsgeräte).

2) Solution of C.36 from Stereotyped Beginnings

Let us assume the beginning "Confidential". From this clear text word and the corresponding encoded text the first twelve jumps of the typing wheel can be deduced. Thus the first twelve peg arrangements of the five wheels are known, if the initial position of the wheels is assumed to be "Zero position"(see Appendix, fig.1)

In fig. 4(see appendix) the five wheels are indicated as having turned with the periods 17, 19, 21, 23, and 25.In the squares containing the sign "X" the peg arrangements of the wheels are known from the clear-encoded compromise,(Klar-Geheim)Kompromiss).The position 26 sign to 29 sign can then be immediately written in the clear text. The continuation is guessed. In this way further peg arrangements in the individual wheels can be determined. These peg arrangements by themselves show pieces of clear texts, etc.at other positions until all peg arrangements are known.

Even wrong solutions of the peg arrangement can be put right by comparing the same wheel position at other positions of the encoded text.The determination of the pegs can aldo be achieved with fairly short positions which have been solved even though the work is more tedious.

3) General Solution of C.36

For the general solution of C.36 an encoded text of considerable length or several short encoded texts are required.

In order to determine the peg arrangement of the wheel with period 17 the encoded text is written in lines 17 long. Thus 17 columns result, and the problem is to divide the 17 columns into two classes in such a way that one class contains the columns in which wheel 17 had a peg active and in other class contains the columns in which wheel 17 had a peg inactive.

This division into classes in a fairly long encoded text can be done by comparing the frequency curves of the individual columns. In German clear texts the max. frequency of E and N cause the appearance of two "hills" in the frequency curves of the columns. Both these "hills" appear in each column. In one class however, the hills are shifted when compared with the hills of the other class at just as many places as the fixed pegs of the rods of the rod cylinder(Stangenkorb) are opposite wheel 17.

Sudoess is achieved in fairly short encoded texts by the elementary theory of errors (Ausgleichsrechnung). The same is done with the four remaining wheels. In this way the peg arrangements of the five wheels are determined. Experience shows that division into classes is done more quickly and with greater certainty the more fixed pegs on the rod cylinder are opposite the wheel in question. If the peg arrangement of a wheel has been solved then it is best to eliminate this wheel from the encoded text etc. If, for example, the peg arrangement of wheel 17(one fixed peg on the rod cylinder lies opposite it) cannot be established, then the encoded text eliminated from the other wheels is written down and under it a second encoded text which results from the first by writing under each letter of the first text the next letter of the alphabet. From both lines the clear text can then be read easily.

4) General solution of BC.38

In principle the general solution of BC.38 is the same as that of C.36. Division into classes, however, cannot be done by elementary mathematical methods. The text must also be much longer; With the aid of Pearson's x^2 = method the solution of a German example text of 5000 elements was possible. It must, however, be stated here that the working is very tedious andthat the solution of the German example was perhaps only possible because each part solution could be confirmed as to whether it was right or wrong.

5) Solution of messages of the same phase with BC. 38

This solution is done by the same procedure as that of C.36. It cannot be remembered whether the determination of the fixed pegs on the rod cylinder was possible; for this work was done at the deciphering center of the Army(Heer). In our opinion the determination of this, even if it should be at all possible, appears to be very difficult and to demand a lot of time, since the shift steps(Verschiebungsschritte) do not lead to one and only one solution of the required peg arrangement, since each rod can have two fixed pegs and also nothing is known a priori about the numbers of the fixed pegs which are opposite the individual wheels.

6) Solution of BC.38 because of an error in wheel setting

This solution was also carried out practically at the deciphering center of the Army.

On occasions in encoding a message one of the six wheels was set wrongly. Then the message was repeated with the correct wheel setting. Such cases could be recognised by the almost identical indicators. If one encoded text is written underneath the other, and if the distances of each pair of letters was established, then the period of e.g. 19 was shown.

From this period the peg arrangement of wheel 19 could be very easily determined and the first encoded text, in which the mistake had been made, could be reduced to the second. In most cases, however, both texts did not correspond completely. This was because the encoder in encoding a clear text twice nearly always makes alterations in the text. One letter is left out or there is some similar omission. In this way, after the reduction of the wrong text to the correct text, two messages of equal phase resulted, the solution of which is described above. The solution of such messages of equal phase was indeed essentially easier, as that both had the same clear text only shifted in phase.

SOLUTION OF TELE-TINTER CIPHER MACHINE T 52 a/b.

1) Cipher principle.

T 52 a/b encodes the signs of the international, five-impulse alphabet. Each sign consists of five impulses apart from the start and stop impulse. Each impulse can be (+) or (-). There are 32 different signs.

In the encoding procedure the individual impulses are at first changed and then transposed. Changing (Tauschung) and transposition (Verwirfelung) are carried out with 10 peg (Nocken)wheels. These ten peg wheels, all have different periods(Teilligkeiten). The pegs are firmly fixed to the wheels. A schematic diagram of the key principle is seen in Fig.5 (see appendix). The positions A,B,C,D,E are the change positions, positions F,G,H,I,K are the transposition positions. With the aid of 10 pairs of stecker wires the 10 peg wheels were connected to these positions. That was the basic or key (Grundschlüssel).

The peg wheel which for example was connected to position A changed therefore the first impulse of the clear sign,i.e.when the peg wheel had a peg active the impulse was changed,(+) became(-) and (-) became(+). The peg wheel transposed the 1 and 5 impulse, i.e. when the peg wheel had a peg active the first proceeded as the fifth impulse and 5 impulse as 1 impulse. When the peg wheel had no peg active then no changing or transposition took place. Each of the 10 wheels moved one step for every letter typed. The movement was therefore uniform.

2) Weaknesses of this cipher principle.

a) The + and - impulses for each of the 5 impulses of the clear signs of the 5 impulse alphabet in the German language are not distributed equally. In some cases the differences are very great,e.g. the 5 impulse has only 27%(+) impulses.

b) Transposition is not very uniform. Assuming that the peg wheels have 50% active pegs and 50% pegs non-active-this is roughly th case- then the distribution of the 5 impulses after transposition is represented by the following table.(See appendix,fig.6)

From 1 impulse therefore:

9	parts	go	to	1)
9	"	"	"	2)
2	"	"	"	3) Impulse after transposition
4	"	"	"	4)
8	"	"	"	5)

The 2 impulse can never appear as 4 and 5 impulse.

c) The arrangement of the pegs (Nockenbestückung) is fixed and this must be assumed as known by the enemy.

d) The movement of the peg wheels proceeds uniformly,in spite of the very long total perios there are 10 short sub-periods corresponding to the period of the wheels.

3) Solution of an encoded text.

a) Given an encoded text of 1000 letters. The encoded text must be available as a perforated strip, i.e. with all signs transmitted.The following must be determined :

i) The day key, i.e. the connection of positions A-K with the wheels.
ii) The indicator (Spruchschlüssel), i.e. the initial position (Ausgangsstellung) of the 10 wheels.

At first the order and initial position of the changing wheels must be determined. Let us assume that the wheel with perios 47 is any one of the changing wheels. The encoded text is written in the period of 47. The sum of (+) impulses,i.e. the number of holes for each sign is written in every field. In this manner 47 columns result 21 in depth(with 1000 encoded signs). In the 47 solumns the numbers of (+) impulses in each field are added. Then a row of 47 numbers results. Since in each of the 5 impulses the number of (+) impulse in German clear texts is not 50%, then the 47 columns can be divided into two classes. To the first class belong the columns which result from active pegs of wheel 47 and in the other class are columns which

result from non-active pegs of the wheel. Since it is known how many pegs wheel 47 has- it may have 24- then the 24 highest numbers are designated "active peg"(Nocke) and the 25 remaining "non-active peg"(Nichtnocke). If wheel 47 is a changing wheel then its place can be found by comparing it with the row of figures formed. It is of no importance if one or the other figures in a column has led to a wrong result. In this way therefore the 5 wheels which were used as changing wheels can be found and at the same time their initial position. It is, however, not yet known to which positions A,B,C,D,E the wheels are connected. Let us assume that wheel 47 was connected to position B. According to Fig.6, this wheel is obvious in the third row of encoded impulses; for 50% of the 2 clear impulse go over into the 3 encoded impulse and the 2 clear impulse has an unequal distribution of(+) and (-) impulses. In this manner the position of the 5 changing wheels which have been found can be determined.

The distribution and the phase of the transposition wheels still remain to be determined.

If peg wheel 53 is connected to I, then the third encoded impulse will be written in phase 53. In half of the columns thus resulting, then changing wheel B_1 which has already been determined, must be found again. If it is not found again, then wheel 53 cannot be connected to position I. With a limited number of attempts the position and phase of the transposition wheels can therefore also be determined. In this way day key and indicators are solved. Any further solution on the same day is essentially easier as only the determination of the new phases of the wheels is now necessary. It should be mentioned here that for this method it is not necessary to assume that the peg arrangement of the wheels is known. The determination at the same time of the peg arrangement can also be achieved from an encoded text of 2000-3000 signs. Several encoded texts which together have 2000-3000 elements may also be used for the solution. In this case the individual messages must "vergattert" in the sub-periods of the wheel periods, i.e. messages with the same indicators listed together.

b) Another solution is also possible. An encoded text of less than 1000 elements is required. In order to determine changing wheel B and transposition wheel I only the third encoded impulse is investigated. Because of the circuit and the fact that the (+) and (-) signs of the clear impulses are unequal in number, wheel B must become obvious. The third encoded impulse is therefore allowed to run through all 10 wheels in turn in each phase. One position then will show the greatest number of coinciding signs. In this way the period and phase of wheel B are determined. After B is known the period and phase of transposition wheel F are correspondingly determined. Similar considerations lead to the determination of the other wheels. This solution, which has only been touched upon, cannot be carried out successfully within a reasonable time without the necessary deciphering apparatus (Entzifferungshilfsgeräte). With apparatus especially constructed for this purpose the solution is possible.

c) T 52 a/b was equipped with a handle which served the purpose of turning back all the 10 wheels to their initial position (indicator). According to the regulations laid down this handle was to be used when the two machines (receiver and transmitter) no longer synchronised. In cases where there were bad conditions of transmission, this was to be expected many times during the transmission of one message.

Since however the number of substitutions in the machine is limited and since these substitutions are known, then the solution of messages of the same phase, which result from making use of the handle, is quite elementary. Probably 5 messages and/or parts (Teile) are sufficient.

If one further considers that in military texts stereotyped beginnings appear particularly frequently, then this solution will have been possible in most cases even without having to employ the general solution methods as under a) and/or b).

4) Change of the transposition pyramid.

Fig. 5 shows the basic transposition pyramid. Other pyramids were, however, possible. In fig. 5 the final points of the transposition switches (Würfelschalter) are numbered 1,2; 3,4; 5,6; 7,8; and 9,10. Fig. 7 shows another transposition pyramid.

5 impulses can be transposed in 5! = 120 different ways. Theoretically therefore a large number of different pyramids is possible. Some pyramids, however, were forbidden. The connections 1,10 or 2,3 or 4,5 or 6,7 or 8,9 were not permissible, as these connections are not effective. A uniform distribution of impulses on the 5 channels is not achieved by any other pyramid. The result therefore as shown in fig. 6 remains in principle and therefore the possibilities of solution as stated also remain. It can become more difficult because in any case a certain number of attempts must be made.

SOLUTION OF TELEPRINTER CIPHER MACHINE T 52 C

1) General Remarks

Since SFM T 52 a/b was considered breakable then the following alterations were proposed by Chi:

a) The use of a 5 impulse alphabet formed according to cryptographic requirements.

b) Changeable pegs on the peg wheels.

c) Ununiform turning of peg wheels.

None of these demands was accepted. Then T 52 C originated. Its only advantage compared with T 52 a/b was that short subperiods no longer appeared.

2) Cipher Principle:

Fig. 8 represents the cipher principle of T 52 C schematically (see appendix). This principle is different from that of T 52 a/b in two points:

a) Where in T 52 a/b one peg wheel is active, T 52 C has four active.

b) While with T 52 a/b there are different transposition pyramids, the transposition pyramid of T 52 C is fixed.

In the case of T 52 C forty positions are influenced by 10 peg wheels. In the first model of T 52 C each peg wheel was used four times, viz twice for changing and twice for transposing. In Fig. 8 therefore each of the 10 positions A to K is changed twice and transposed twice. The letters written in the diagram were chosen at random so that they can only be taken as a representation of the principle.

3) Possibility of breaking into this circuit.

Since each of the peg wheels takes part in the changing twice (compare Fig. 8) the clear sign is changed by the changing process in a characteristic manner. Let us assume that the clear sign had 3+ and 2- impulses. By the changing process either two of the three + impulses are changed by a peg wheel resulting in one + and four - impulses or the two - impulses are changed resulting in five + and 0 - impulses or finally one + and one - impulses are changed resulting in three + and two - impulses. In other words: the number of the + impulses always remains odd and the number of the - impulses always remains even when the effect of a wheel on the changing process is taken into consideration. In general terms: by the changing process the even and odd character of the + and/or - impulses of the clear sign is not changed.

By transposition the character of the impulses is not changed, therefore the encoded sign has just as many + and/or - impulses modulo 2 as the clear sign.

If in a text a clear word is presumed then it is known for example how many + impulses each letter of this word has in the five impulse alphabet. If the letter sequence is written down as a row of figures mod 2 then a sequence of figures 0 and 1 results e.g. 001011101100 from a word of twelve letters. In the encoded text all signs are now written down according to the number of + impulses. Thus a sequence of figures of 0 and 1 also results here. The sequence of figures of the presumed clear text word is then moved along the sequence of figures of the encoded text. If at any one position of the encoded text the same figures appear it can be concluded with great probability that the presumed clear text word is at this position of the encoded text. The longer the word the less probability that a similar place in the sequence of figures of the encoded text

results from another clear text word. Thus a part compromise of clear and encoded text has originated. The uniform turning of the peg wheels, the fixed peg arrangement and the method of working of the machine just described must be considered as such great weaknesses that the discovery of a method of solution would have to be reckoned with sooner or later.

A change of circuit was therefore made. Each wheel was no longer used twice for changing and twice for transposing. Some wheels could even be used three times for changing and once for transposing and vice versa. Instead of in Fig. 1 some letters would appear at the changing position 3 times and/or once; similarly at the transposing position.

This the possibility of guessing places of clear text was done away with. The Security investigations were continued. Meanwhile the different decipherting machines (Enziffermaschilfsgeräte) had shown their worth in solving cryptographic problems. Experiences had been gained particularly about the good work of those deciphering aids even at high speeds. With these prerequisites it was possible to give a method with which T 52 C could be solved by employing deciphering machines. !!!

4) General Solution of T 52 C

The basic idea of the solution is as follows:
The transposition pyramid divides each individual impulse non uniformly on the five channels. Fig. 6 represents the division of each impulse on the five channels. 50% of the second impulse after transposition proceeds along the third channel, 50% of the third impulse along the fourth channel and 50% of the fourth impulse along the first channel. If on the typewriter of T 52 a/b or C the "Letter Key" is always pressed (in the five impulse alphabet this consists of 5 + sigma) then the changing wheels in the second channel become 50% obvious in the encoded text of the third channel.

Of the remaining 50%, half correspond with the changing wheels owing to accidental distribution. In the second channel therefore the changing wheels become 75% obvious in the encoded text of the third channel. Since from the clear text no equal distribution of + and - impulses goes into the machine, the changing wheels of the second channel become more than 50% obvious in the third sequence of encoded impulses. Similarly for the changing wheels in the third and fourth channels which become obvious from the sequence of encoded impulses of the fourth and fifth channels. These facts lead to a solution:
From ten different peg wheels $\frac{10 \times 9 \times 8 \times 7}{1 \times 2 \times 3 \times 4} = 210$ different combinations, each consisting of four wheels, can be formed. One of these 210 different combinations must therefore be effective as the changing wheels combination e.g. in a second channel during the encoding of the text to be solved. The problem is to find this combination and at the same time to determine the correct phase position of the wheels. For this purpose a sequence of impulses from each of the 210 different combinations is formed. This sequence must be as long as the period of the four wheels used on this occasion. The third sequence of impulses of the encoded text, which is to be solved, will be now compared with each of the 210 different sequences of impulses to see which impulses correspond. A maximum of cases of correspondence will be offered by the right combination in the right phase position. These investigations can only be made with quick working deciphering machines.

If e.g. a combination of the changing wheels is found in the second impulse then the determination of the changing wheel combinations in the third and fourth impulse is essentially easier.

In this manner the peg wheels which are effective as changing wheels in the second, third and fourth channels are determined. For the most part these are at least nine wheels. The last missing wheel can then be found easily by trial and error.

5) Further development of SFM T 52

After these conclusions had been arrived at it was decided to introduce ununiform turning of the wheels, in order to prevent the possibility of solution by the appearance of subperiods. Thus by reconstructing T 52 a/b the types T 52 D originated and from T 52 C the type T 52 E originated. Types D and E are characterised by ununiform turnings of the peg wheels. In the case of both these types up to now no possibility of solution has been seen.

For the sake of completeness it must be stated here that in the case of all types of T 52 the solution of messages of equal phase is of course possible. For this purpose in practice about ten messages of equal phase will be necessary.

SOLUTION OF SFMT 43 BY REASON OF TECHNICAL DEFECTS OF THE MACHINE.

1) Encoding with SFMT 43 is effected by the superposition of a Key perforated strip on the clear perforated strip, which results in a pure addition of clear and key impulses in accordance with the following principle:

Equal current conditions in the clear - and key sign give a + impulse in the encoded sign and unequal conditions give a - impulse.

$$\begin{matrix}(+) + (+) = (+)\\(-) + (-) = (+)\\(+) + (-) = (-)\\(-) + (+) = (-)\end{matrix}$$

(The reverse may have been the case)

This corresponds to the scheme: (See Fig. 9 in appendix.)

2) Each key perforated strip is only used once, so that the solution of an encoded text is thus theoretically impossible. The key perforated strip is automatically destroyed after it has passed through the machine.

3) Defects of the machine, which schematically have exactly the same result as a phase- shift in the superposition of clear and key signs, are key relays, which work too slowly. Eg The phase shift from key sign to clear sign is 30%. (This is naturally less in practice.)

An oscillogram of encoded texts showed therefore shortened and lengthened impulses. In order to remove this defect it was demanded that every SFMT43 be coupled with a so-called teleprinter "Entzerrer" which synchronised the encoded impulses. It cannot be stated with certainty whether everywhere, where SFMT43 was used, the teleprinter "Entzerrer" was actually employed. Siemens made every effort to remove the sources of technical defects by changing the construction of SFMT43. New perfect machines however never came into action.

4) One and only one solution of an encoded text with non-synchronised impulses by making use of an oscillogram is possible. In example fig. 10 (see appendix) the first gap in the current (a) in the encoded sign must result from a + impulse in the key sign. Since the first encoded impulse and the first key impulse are both + then the first clear impulse must be +. In addition the second key impulse must be + for otherwise the first encoded sign would have been shortened. Since the second encoded impulse is - then the second clear impulse must be -. Since further the second encoded impulse is shortened the third key impulse must be -. In this way further conclusions can be arrived at and one and only one solution of clear and key signs be found.

SZ 40 AND SZ 42A and B

1. General Remarks

In 1937 the development of an automatic Schlüssel-Zusatz was begun by Heeres Waffenamt (WA Prüf 7). Firm Lorenz AG was commissioned to undertake the technical work. The principle of a Zusatz was chosen so that it could be connected to any clear teleprinter. The Zusatz was to function mechanically as opposed to the teleprinter cipher machine T.52 which worked electrically.

Throughout the years different types of Zusatz were developed, constructed and put into service: SZ 40 (old type), SZ 40, SZ 42a, SZ 42b, SZ 42c; the last one was not completed at the end of the war.

Investigations of the security of the different Zusätze were undertaken by Uffz Dr LINDMAYER (OKH/AgN, since autumn 44 OKW/Chi), and Lt Dr STEIN (OKW/Chi). These are the only two who are able to give detailed information about the security or solution of the Zusätze. The statements made here can therefore lay no claim to completeness and in part no claim to absolute reliability.

2. SZ 40 (old type).

With SZ 40 (old type) the impulses of the five impulse alphabet were changed. Two of the ten peg wheels influenced one impulse. The peg wheels had fixed pegs. Each wheel moved one step for every letter. The periods of the wheels had no common factor. The periods were about 90 long.

The security of this type was not great:

a) two messages of equal phase could be solved according to the same principle as two messages of, e.g. C.36 (Hagelin).

b) the indicator could be obtained from a part compromise. Since the period and peg arrangement had to be assumed as known by the enemy, then the so-called "pure key" of the machine could be deduced. Under "pure key" the encoded text is understood which comes out of the machine when as clear text the "letter key" is always pressed. Since the 5 impulse sign of the "letter key" consists of nothing but + impulses then the "pure key" offers to some extent a representation of the effect of the peg arrangement. If with SZ 40 (old type) the "pure keys" for each of the five impulses are formed (each of these five keys has a length of roughly 90 x 90 = 8100 signs) then in each of these five keys the position must be found again, which is identical with the "pure key" of the part compromise. In doing this the "pure key" of the part compromise is obtained by subtracting the clear text from the encoded text. In this manner the phase position of the peg wheels is found at the moment of the encoding of the compromise text. Thus the indicator is found and the entire encoded text can be decoded.

c) An individual encoded text of 1000 - 2000 elements could be solved. The first sequence of impulses of the encoded text results by the superposition of the "pure key" of the first impulse over the clear text. The "pure key" of an impulse on the other hand results from the superposition of two peg wheels. If, therefore, the first row of encoded impulses is written in rows equal in length to the period of a peg wheel, then the individual columns contain impulses which were treated equally by this peg wheel, i.e. all with actove peg or all with inactive peg. Since the clear text shows no equal distribution of + and - impulses then the peg arrangement of the other peg wheel which was active during the encoding becomes obvious.

For these reasons SZ 40 (old type) was only constructed in small numbers (roughly 40 models) and was only employed for short periods on land lines which could be checked. SZ 40 was then developed from this first model.

3. SZ 40.

SZ 40 has twelve peg wheels of different periods with variable pegs. Fig. 11 gives a schematic representation of the method of working of the machine. (See Appendix). The twelve peg wheels are given the letters A - M. The periods are given in brackets. Each of the Spaltenclear wheels (H - M) moves one step for every letter. The Springclear wheels either move one step together or they do not move. The movement of the Springclear wheels is controlled by the Vorgelege. This control is effective according to the following rule: For every letter wheel G moves one step. Wheel F then moves a step whenever an active peg of wheel G comes into play. The Springclear wheels then move one step together when an active peg of wheel F comes into play.

The peg wheels A and H encode the first clear impulse, B and I the second, C and K the third, D and L the fourth, and G and M the fifth. Dissimilarity of peg conditions in one of the pairs of wheels leads to a change of the clear impulses, i.e. + becomes - and vice versa. Similarity of peg conditions in a pair of wheels makes the clear impulse remain unchanged.

At first, after introduction of SZ 40, the Spalten- and Springclear wheels were given a new peg arrangement monthly and the Vorgelege wheels daily. The twelve peg wheels were turned to a different basic position for each message. Recently all twelve peg wheels received a new peg arrangement daily.

Security of SZ 40.

a) Two messages of equal phase can be solved according to the same method of two messages of equal phase with SZ 40 (old type). After solution of messages of equal phase the whole machine can be solved as follows:

If the corresponding clear text is subtracted from one of the solved encoded texts, then the "pure key" results. The first row of impulses of impulses of this "pure key" is written in lines 41 long, one under the other. The number of changes which appear between neighbouring impulses of the first and second column is now determined. Such a change is evident when in the first column a + appears and in the second column next to it a - or vice versa. Similarly the number of changes between the second and third column, the third and fourth column etc to finally between the forty-first and first column are arrived at. If the number of changes in one column is greater than half the depth of the column, then at this position a peg change has taken place in the Spaltenclear wheel H (41). If the number is less than half the depth of the column, then no peg change has taken place. This results in the following manner:

The Springclear wheels on many occasions do not move during the encoding of some signs; then no change of impulse can be caused by the Springclear. If a change of impulse is present then it must have been caused by the Spaltenclear. In this manner, therefore, the peg arrangement of wheel H can be determined. At one position an assumption must be made as to whether a peg is active or inactive in wheel H. If this assumption is wrong, then the reverse of the peg arrangement results. This is, however, unimportant, as later the reverse of the peg arrangement can be found from the corresponding Springclear wheel A.

Similarly the peg arrangements of other Spaltenclear wheels I,K,L,M are found.

Simultaneously with the peg arrangement a relative phase of the Spaltenc&aumlsar wheels is determined. If the "pure key" is eliminated from the Spaltenc&aumlsar by subtraction, then the pure Springc&aumlsar key remains. The task remains to determine from the pure Springc&aumlsar key the peg arrangement of the Springc&aumlsar wheels and the Vorgelege wheels.

For this purpose the complete five impulse signs of the pure Springc&aumlsar key are required. Since all five Springc&aumlsar wheels often do not move, then the pure Springc&aumlsar key is characterised by the fact that frequently similar five impulse signs follow immediately after one another. In order to determine the positions at which the Springc&aumlsar wheels have moved one step, vertical lines are drawn between the signs at each position at which at least one impulse has changed from one sign to the other. It may be that lines will have to be drawn also between two signs which look the same. Then at these positions the peg wheels of the Springc&aumlsar have moved one step but the peg character of each Springc&aumlsar wheel has in doing this not altered. Since the periods of the wheels are known then by a few attempts the correct jumps can be determined. The peg arrangements of the Springc&aumlsar wheels and their relative initial positions are thus known. The arrangement of the Vorgelege wheels still remains to be determined. By the marking off in the "pure Springc&aumlsar key" the positions are known at which stop orders were given by the Vorgelege. From the sequence of these stop orders, the knowledge of the periods of the Vorgelege wheels and the move mechanism of these wheels, the peg arrangements can easily be determined.

Thus the entire machine setting is solved, and the longer of the two encoded texts can be encoded to the end.

b) The description of the solution of the peg arrangements from two messages of equal phase shows at the same time how the machine setting can be solved from a clear - encoded - compromise.

c) It is known that the above-mentioned G-Zus&aumltze experts recognised a weakness of the machine in the comparatively short period of the Vorgele (this period equals 37 x 61 = 2257 steps). In the case of a long encoded text of about 20,000 encoded letters the period of the Vorgelege and thus the drive of the Springc&aumlsar wheels appears ten times. This fact led to their making statements concerning the stop orders of the Vorgelege. Details of these are not known.

d) At the beginning of the employment of G-Zus&aumltze it was normal to press the "letter key" at the beginning of each message. When the indicator of many messages (about 120) was known and also the first clear sign of each, the peg arrangement could be solved. Details can no longer be given.

In order to prevent all these possibilities of solution, series of regulations were issued. It was forbidden to press the "letter key" as the first sign. Nonsense words were to be placed at the beginning and the end of each message, i.e. words chosen at random by the encoder and which had nothing at all to do with the contents of the message. The length of messages was limited to 10,000(?) letters. In addition regulations for peg arrangements were worked out and employed which were to prevent the solution described under para a) and any similar solutions. (The regulations for peg arrangements will be gone into in more detail under the description of SZ 42).

After these regulations which, however, made procedure much more difficult, SZ 40 was considered as secure.

In the meantime a technical alteration had also been envisaged for SZ 40, which was to make the turning of the Vorgelege more complicated. In this way SZ 42A and SZ 42B originated.

4. SZ 42A and B.

The difference between SZ 42A and B and SZ 40 was only in a change of the method of drive of the Springoßsar wheels. In the case of SZ 42A the fifth impulse of the clear text and the peg arrangement of wheel I, influenced the drive of the Springoßsar wheels as also did both Vorgelege wheels. In the case of SZ 42B wheel A of the Springoßsar also came into play. It may be mentioned here that the change from SZ 42A to SZ 42B was not made for reasons of deciphering security but comes from technical proposals made by Dr LIEBKNECHT of WA Prüf 7.

The clear text function was introduced in order to prevent the appearance of messages of equal phase. The result of further security investigations made by the above-mentioned experts was the recognition of further weaknesses, details of which are no longer known by FW. It can be said with certainty that these weaknesses could be done away with by a suitable choice of peg arrangements. Therefore, peg arrangement regulations for SZ 40 and SZ 42 were worked out by the above-mentioned experts. The peg arrangement regulations consist of lists of tables which are given to the producer of the key.

The lists of tables can be described as follows:

1) Peg sequences 1, 2, 3 or 4 long were allowed generally for each wheel, i.e. at the most four similar peg conditions were allowed to follow one another.

2) The limit of the number of active pegs was given for each wheel.

3) The limit of the number of peg sequences was given for each wheel.

It was left to the producer of the key to decide into which sequence he arranged the peg sequences. This sequence was chosen by him out of the hat.

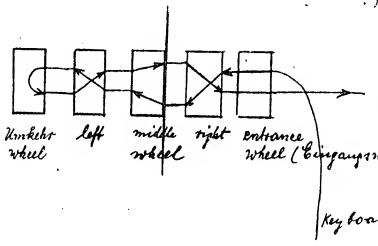
Fig. 12 (See Appendix) shows the layout of one table, as far as it is remembered by FW. It serves to provide the arrangement of wheel H (41). In the left column are the numbers of active pegs which are allowed. Along the top are the peg sequences allowed. In the table itself each line gives, under the peg sequences allowed, two lots of four numbers. The producer of the key chooses one of the peg numbers, for example 17. He then chooses to the right of 17 in the table one of the rows of figures, e.g. 4311 1332. The peg arrangement of wheel H (41) shows therefore four isolated +, three peg sequences ++, one peg sequence +++, one peg sequence ++++, one isolated peg -, three peg sequences --, three peg sequences ---, and two peg sequences ----. The sequence is chosen out of the hat. The result is, e.g. ++ --- + -- +++ ---- ++ -- + - + ---- ++ ---- ++++ ---- + --. Similarly from the tables the peg arrangements of all Spalten - and Vorgelege wheels were taken. After determining the arrangements of the Vorgelege wheels the choice in the table for the arrangement of Springoßsar wheels was limited.

5. SZ 42C

The plans for SZ 42C represent another step in the development of G-Zusätze. Here also the Spaltenoßsar wheels were to move ununiformly and indeed each one individually. The control of the Springoßsar wheels was to be taken over by the Spaltenoßsar wheels so that both Vorgelege wheels dropped out. This development, however, was never concluded.

Appendix (Solutions of Enigma machines)

Fig 1. – Enigma K –



		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
1	a	06	11	25	05	15	04	08	22	14	01	18	15	24	03												
2	b	12	26	06	16	05	09	23	15	05	19	16	25	04	20												
3	c	01	07	17	06	10	24	16	06	20	17	26	05	21	04												
4	d	08	18	07	11	25	17	07	21	18	01	06	22	05	07												
5	e	19	08	12	26	18	08	22	19	02	07	23	06	08	24												
6	f	09	13	01	19	09	23	20	03	08	24	07	09	25	02												
7	g	14	02	20	10	24	21	04	09	25	08	10	26	03	05												
8	h	03	21	11	25	22	05	10	26	09	11	01	04	06	18												
9	i	22	12	26	23	06	11	01	10	12	02	05	07	19	08												
10	j	13	01	24	07	12	02	11	13	03	06	08	20	09	17												
11	k	02	25	08	13	03	12	14	04	07	09	21	10	18	10												
12	l	26	09	14	04	13	15	05	08	10	22	11	19	11	11												
13	m	10	15	05	14	16	06	09	11	23	12	20	12	12	12												
14	n	16	06	15	17	07	10	12	24	13	21	13	13	13	19												
15	o	07	16	18	08	11	13	25	14	22	14	14	14	20	25												
16	p	17	19	09	12	14	26	15	23	15	15	15	21	26	14												
17	q	20	10	13	15	01	16	24	16	16	16	22	01	15	21												
18	r	11	14	16	02	17	25	17	17	17	23	02	16	22	06												
19	s	15	17	03	18	26	18	18	18	24	03	17	23	07	22												
20	t	18	04	19	01	19	19	19	25	04	18	24	08	23	01												
21	u	05	20	02	20	20	20	26	05	19	25	09	24	02	16												
22	v	21	03	21	21	21	01	06	20	26	10	25	03	17	09												
23	w	04	22	22	22	02	07	21	01	11	26	04	18	10	26												
24	x	23	23	23	03	08	22	02	12	01	05	19	11	01	15												
25	y	24	24	04	09	23	03	13	02	06	20	12	02	16	13												
26	z	25	05	10	24	24	14	03	07	21	13	03	17	14	23												

etc.

Figure 2

FIG. 2

Figure 3.

Clear Text.

	g	a	b	i	n	e	t	t	o	a	l	t
	14	11	06	23	07	08	19	25	22	04	11	08
	02	25	16	06	10	22	25	04	14	18	19	23
x	20	05	05	11	12	19	04	18	14	15	11	01
	10	15	09	01	24	02	18	24	14	24	11	15

etc.

Encoded Text.

	z	s	e	w	g	j	i	x	j	p	s	u
	25	17	12	22	24	02	01	12	03	15	17	24
	05	03	26	02	21	11	10	01	06	15	23	02
x	10	18	18	07	04	13	12	05	08	21	07	16
	24	26	08	21	09	03	02	19	20	26	22	08

etc.

FIG. 3

Figure 4

Appendix (Solution of Hagelin machines).

Fig. 4

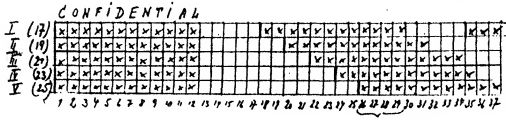
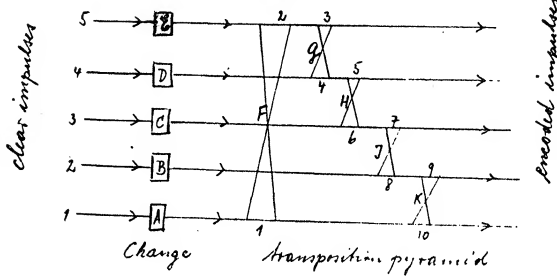


Figure 5

Appendix (T 52a/b)

Fig. 5.



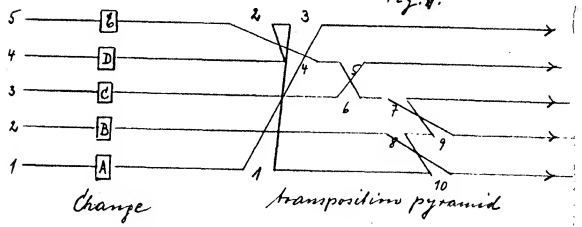
out

inp.	1	2	3	4	5	inp.
1	9	9	2	4	8	
2	8	8	16	–	–	
3	4	4	8	16	–	
4	2	2	4	8	16	
5	9	9	2	4	8	

in

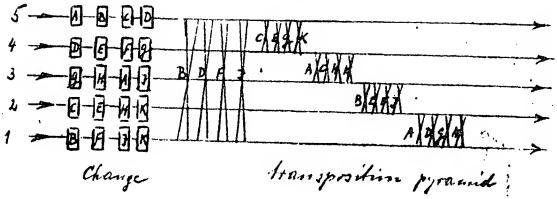
Fig. 6

Fig. 7.



Appendix (T52.c)

Fig. 8.



Appendix (SFHP43)

Fig. 9

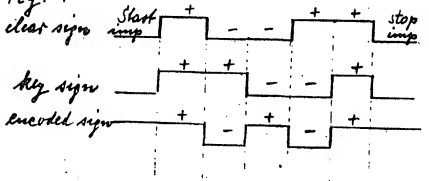


Fig. 10

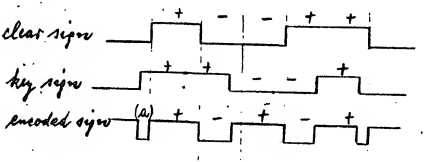


Fig 11 and 12

I-45

Appendix (Schlüsselzusätze)

Fig 11

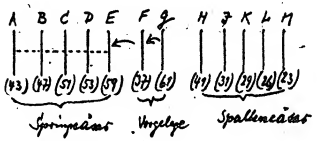


Fig 12.

Wheel H (47)

	+ + + + + +	− = ≡ ≡
17	4 3 1 1 etc.	1 3 3 2 etc
18		
etc (f.e. 23)		